


RESEARCH

Open Access



Anti-jamming for cognitive radio networks with Stackelberg game-assisted DSSS approach

Muhammad Imran¹, Pan Zhiwen^{1,2*}, Liu Nan¹, Muhammad Sajjad³  and Faisal Mehmood Butt⁴

*Correspondence:
pzw@seu.edu.cn

¹ National Mobile
Communications Research
Laboratory, Southeast University,
Nanjing 210096, China

² Purple Mountain Laboratories, 9
Mozhou E Rd Jiangning District,
Nanjing, Jiangsu, China

³ Department of Electrical
Engineering, Iqra National
University, Peshawar 25100,
Pakistan

⁴ Department of Electrical
Engineering, University
of Azad Jammu and Kashmir,
Muzaffarabad, Pakistan

Abstract

The proposed study introduces a novel anti-jamming approach for cognitive radio networks (CRNs) by integrating the Stackelberg game model with direct sequence spread spectrum (DSSS) techniques. This innovative combination enhances the security and performance of CRNs by optimizing resource allocation and fortifying network resilience against jamming attacks. The Stackelberg game model provides a strategic framework where the Defender and Adversary dynamically adjust their strategies to achieve Nash equilibrium, ensuring strategic stability. The application of DSSS further improves signal robustness, mitigating interference from jamming attempts. Simulation results demonstrate significant improvements in network security, resource utilization, and overall performance, validating the efficacy and advantages of the proposed scheme in maintaining reliable communication in the presence of adversarial threats.

Keywords: Cognitive radio networks, Resource allocation, Network security, Anti-jamming, DSSS, Stackelberg game

1 Introduction

Cognitive radio networks are designed to opportunistically access underutilized spectrum bands while coexisting with incumbent users and other cognitive radios. However, they are susceptible to jamming attacks, which can disrupt communications and compromise network performance. Anti-jamming methodologies are crucial for ensuring reliable and secure communication in these dynamic and congested wireless environments.

To address this concern, machine learning and statistical analysis-based intrusion detection systems can be deployed. Change point detection techniques enhance cognitive radio systems' security, while cooperative localization strategies help adjust transmission power to avoid interference with primary users. These methodologies significantly contribute to the dependability and security of cognitive radio networks [1].

A combination of various methodologies, such as spectrum sensing (SS) detection, change point detection methods, and deep reinforcement learning (DRL), can effectively mitigate jamming attacks. SS detection techniques, including matched filter detection, cyclo-stationary feature detection, and hybrid filter detection with inverse covariance, accurately identify user presence at low-power levels [2]. Change point detection



© The Author(s) 2024. **Open Access** This article is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License, which permits any non-commercial use, sharing, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if you modified the licensed material. You do not have permission under this licence to share adapted material derived from this article or parts of it. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

methods enhance security by detecting intrusions, while DRL algorithms adapt to behavioral changes of secondary users (SUs) during cooperative spectrum sensing (CSS), reducing sensing errors.

Developing robust strategies to counter jamming attacks is critical for maintaining service continuity, network capacity, and user satisfaction in critical sectors such as infrastructure, health care, and transportation [3]. Researchers are exploring innovative ways to reduce vulnerability to jamming attacks, including spectrum sensing algorithms, adaptive modulation and coding schemes, collaborative spectrum sensing techniques, and physical layer security measures [4].

In game theory, Stackelberg games provide a valuable framework with non-cooperative models and sequential decision-making processes. This structure is particularly relevant in cognitive radio networks, where anti-jamming techniques are essential. The Stackelberg model captures the dynamics between a network defending against jamming attacks and an Adversary seeking to disrupt it, leading to effective network security [5].

By dynamically adapting spectrum access using the Stackelberg model, cognitive radio networks can create effective countermeasures. This approach ensures the protection and fortification of the network, maintaining uninterrupted data transmission [6].

Cognitive radio networks (CRNs) offer advanced spectrum management but face significant challenges from jamming attacks. Existing strategies, such as power allocation (PA), frequency hopping (FH), and rate adaptation (RA), each contribute to mitigating jamming but have notable limitations. PA methods often lack adaptability, FH strategies can be ineffective against sophisticated jammers, and RA approaches might degrade performance under certain conditions. This study addresses these gaps by integrating game theory with the direct sequence spread spectrum (DSSS) technique to enhance CRN security and performance. By focusing on these advancements, the research aims to provide a more robust solution for countering jamming attacks, surpassing the limitations of previous approaches.

2 Methods/experimental

2.1 Study design

The study uses a quantitative approach based on the Stackelberg model, integrated with direct sequence spread spectrum (DSSS) to enhance the security and performance of cognitive radio networks (CRNs). It focuses on analyzing interactions between Defenders and Adversaries to validate Nash equilibrium as an indicator of strategic stability.

2.2 Setting

Research was conducted in a simulated environment designed to mimic real-world CRNs. This controlled setting allows for the manipulation of variables and observation of outcomes relevant to modern CRNs, including those expected in 5G and beyond.

2.3 Participants and materials

Simulated participants in the study include primary users (legitimate spectrum users) and secondary users (potential jammers). Materials used are:

- Simulation software for modeling CRN dynamics.
- DSSS technology modules for signal dissemination.
- Algorithms for implementing the Stackelberg game model.
- Statistical tools for evaluating Nash equilibrium.

2.4 Interventions and comparisons

The intervention involves applying the DSSS approach within CRNs alongside the Stackelberg game model to assess resilience against jamming. Comparisons include:

- Network performance with and without DSSS.
- Strategic stability (Nash equilibrium) before and after implementing the Stackelberg model.
- Variations in resource allocation and utility under different jamming intensities.

2.5 Analysis

The analysis involves:

- Simulation: Creating scenarios with varying jamming attempts and resource allocations.
- Application: Implementing DSSS and Stackelberg game model to analyze strategic interactions.
- Statistical Evaluation: Analyzing data to identify Nash equilibrium using metrics such as network security, utility, and channel occupancy.
- Validation: Confirming results through multiple simulation runs to ensure consistency and reliability.

3 Literature review

Cognitive radio networks (CRNs) offer efficient spectrum allocation and the potential to enhance various aspects of communication infrastructure. However, with their adaptability comes an array of security concerns, particularly jamming attacks. This literature review examines various anti-jamming approaches and strategies proposed in recent research to address these security challenges and optimize the functionality of CRNs. We can broadly classify them into power adaptation (PA), frequency hopping (FH), rate adaptation (RA), and joint techniques as discussed below:

3.1 Power allocation-based anti-jamming

Game-theoretical PA problems attracted much interesting. The authors in [7] protect the wireless network from jamming attack by presenting an adaptive PA strategy for controlling transmission power of the network nodes. This method updates the network topology by using a scalable decomposition approach which nullifies effects of the jammer. Power distribution has been deemed as an efficient anti-jamming strategy by Gar-naev et al. [8]. The authors provide analytical proofs to validate the presence of Nash equilibrium in a Bayesian jamming game between the jammer and network Defender. A

revolutionary learning approach has been implemented to allocate power in anti-jamming CRNs through the usage of the continuous blotto game (CBG) model [9]. In a study on cognitive radio networks [10], researchers presented a game called leader–follower Stackelberg for anti-jamming defense. The PA problem is split into two sub-sequential problems, i.e., leader sub-game and follower sub-game to reduce the game complexity. Stackelberg game is employed to select optimal relay for securing physical layer communications in the CRNs [11]. For simplicity, a one leader–follower Stackelberg game (OLFSG) is modeled to achieve optimal PA strategy in the presence of eavesdroppers. Likewise, the application of game theory has been proven to be of great significance in the enhancement of PA strategies in dynamic jamming scenarios [9].

3.2 Frequency hopping-based anti-jamming

Chen et al. [12] discussed the challenges in avoiding a malicious jamming attack on CRNs and presented a game-theoretical anti-jamming scheme for jamming and the anti-jamming process. The network users in this scheme proactively hop among accessible channels to avoid the jamming attack. This work is further extended by Khalid et al. [13] for CRNs and cognitive radio-based wireless sensor networks. To study the effect of jamming attack, the authors considered the time variation in wireless channels from one sub-channel to another. Besides, they set up 15 sub-channels in the radio spectrum to analyze the efficacy of FH strategy for the anti-jamming game played on those channels. Wang et al. [14] devised Q-learning aided game-theoretic approach to mitigate a dynamic jamming attack on cognitive radio network. With this approach, the hopping strategy shows a benchmark performance in terms of spectrum efficiency against opponent users of the spectrum. Proactive [15] and reactive FH [16, 17] are two commonly used FH approaches to mitigate jamming for wireless networks. In the proactive FH anti-jamming, the transmitter and receiver proactively hop between channels without verifying state of the channel. Another words, the legitimate transmitter and receiver not needed to detect the presence of a jammer. The legitimate transmitter and receiver in the reactive FH minimize the FH cost by reactively hopping to a new channel if the current channel is jammed. The authors in [18] proposed an uncoordinated FH strategy to alleviate the jamming problem in which the transmitter and receiver perform random FH without using pre-shared keys.

3.3 Rate adaptation-based anti-jamming

Transmission rate adaptation is a typical way of thwarting jammer in wireless networks [19, 20]. In rate adaptation-based anti-jamming, the network users utilize coding sequence to enhance the signal robustness. The DSSS improves signal-to-noise ratio by filtering out the noise signal using pseudo-random chip sequence. RA is suitable for networks having high security requirements [21]. Nevertheless, analysis of optimal jamming strategies against these RA algorithms indicates that the performance can be significantly degraded with an interfering radio frequency signal. In [22], it is shown that a jammer capable of randomizing its power levels can restrict the transmitter to constantly communicate at the lowest transmission rate. While adapting a high transmission rate, on the other hand, increases the chances of disrupting transmission on the

communication channels; whereas, a lower transmission rate increases the signal's robustness to jamming but reduces average throughput of the network.

3.4 Joint anti-jamming

PA [7–11], FH [12–18], and RA [19, 20] based strategies are commonly used to mitigate jamming as argued above. However, anti-jamming techniques based on these strategies when applied separately have shown to be ineffective against deliberate jammers [22–24]. Motivated by this, the authors in [22] studied the ability of a joint PA and RA strategy for mitigating jamming. Likewise, the authors in [25] proposed a joint FH and RA strategy for securing the wireless network users from a reactive sweep jammer attack. Results of these joint anti-jamming exhibit significant improvements in the average throughput and jamming resiliency.

3.5 Evaluation of anti-jamming techniques

Over the past 50 years, the evolution of anti-jamming techniques in communication has progressed from adaptive methods to intelligent solutions, incorporating advancements in game theory and machine learning [26]. Researchers have developed innovative strategies like the bivariate frequency agility (BFA) system, utilizing Markov decision processes and deep deterministic policy gradient algorithms to enhance signal-to-noise ratios in the presence of jamming [27]. Additionally, the introduction of adaptive channel selection (ACS) schemes, such as the VU-ACS, has significantly improved electronic counter-countermeasures (ECCM) capabilities by intelligently selecting jamming-free channels based on wideband spectrum sensing and bit error rate calculations [28]. Furthermore, the utilization of reconfigurable intelligent surfaces (RIS) with angular responses has shown promising results in optimizing channel capacity and anti-jamming performance through complex optimization techniques and algorithms like the alternating direction method of multipliers (ADMM) [29]. To address rapid changes in jamming environments, parallel Q-learning (PQL) and slot cross Q-learning (SCQL) algorithms have been proposed, enabling reliable communication by reducing sensing and learning times [30].

3.6 Motivations and contribution

Extensive research has been undertaken for securing the cognitive radio networks with the PA [7–11], FH [12–18], RA [19, 20], and joint anti-jamming [22, 30] against Adversary attacks. Yet, these approaches mainly improve network efficiency in ideal conditions, without considering interference from neighboring channels or using game theory for anti-jamming strategies. The use of an effective anti-jamming approach is a major research problem for cognitive radio networks and dealing with malicious Adversaries. This research aims to prevent harmful jammers from disrupting cognitive radio networks. Following are the main objectives of this research:

- To propose an effective anti-jamming approach for counter measuring the problem of jamming attacks in cognitive radio network.
- To enhance security and improve resource allocation of the cognitive radio network.

3.6.1 Motivations

Cognitive radio networks may experience resource degradation from jamming attacks, with the degree of degradation varying based on the attacker's strategy. The core problem that underlies this specific investigation is characterized by a dichotomy, encompassing two separate dimensions that collectively augment its intricacy and importance. Firstly, it is of utmost importance to tackle the security challenges that arise as a result of the menacing jamming attacks in cognitive radio networks. These attacks possess the potential to cause severe disruptions to the functionality and performance of CRNs, thus making it an absolute necessity to develop effective strategies to counteract them. Secondly, this study explores game theory as an effective way to reduce the harmful impact of jamming attacks in cognitive radio networks. By harnessing the powerful equilibrium condition of game-theoretic models, strategies, and principles, it becomes plausible to fabricate anti-jamming mechanisms that are not only dynamic but also adaptive in practical deployments, thereby significantly bolstering the security and resilience of cognitive radio networks in the face of any malicious interference that may be encountered.

Research has contributed a lot for providing anti-jamming schemes to secure cognitive radio networks. FH strategy has considered either separately or jointly with RA strategy for mitigating jammer, and no one has considered DSSS and Stackelberg approach together for mitigating the jammer for CRN. To ensure secure communication in cognitive radio networks, an anti-jamming approach assisted by game theory is needed. This approach should take into account communication through adjacent channels in real-life scenarios. The proposed anti-jamming approach has a big advantage. It lets the network users mitigate the jammer by rendering the communication signals and game theoretically changing its tactics. This innovative method combines DSSS and game-theoretic dynamics for robust security.

3.7 Contribution

Using Stackelberg game theory in this study on anti-jamming for cognitive radio networks is justified for several reasons. Game theory helps us understand how Defenders and Adversaries make decisions, which leads to effective anti-jamming strategies. In game theory, the Stackelberg game model and DSSS let Defenders strategically allocate resources. This helps them tip the scales of victory in their favor. It also allows for a detailed exploration of optimal strategies in the dance between opposing players.

- Considering the Adversary is capable of following the Defender strategy, we model the interactions between the Defenders and the jammers as a Stackelberg game. The Stackelberg game approach captures the intricate dynamics between jammers and network coordinators in anti-jamming cognitive radio networks, emphasizing the utmost significance of strategic decision-making in the realm of jamming scenarios.
- This study examines security issues in cognitive radio networks. It focuses on the interactions between network operators and jammers. The application of game theory helps understand and address these issues. Our simulation results

reveal that combining DSSS with the Stackelberg game model for anti-jamming under the constraints of Nash equilibrium maximizes the Defender's utility and improves resource allocation and the cognitive radio network security.

4 System model

In this section, we explain the system model of our anti-jamming method for protecting cognitive radio networks. The system model integrates cognitive radio networks with DSSS and the Stackelberg game-theoretic approach. The proposed method maximizes security with DSSS and optimizes resource allocation using strategic decision-making and the Stackelberg game model. It addresses challenges in cognitive radio networks, particularly in countering jamming attacks while ensuring efficient spectrum utilization.

The spectrum is divided into M -adjacent channels, where all channels are unoccupied initially. The jamming attack is assumed to be the only source of interference in the network, and we ignore other interference effects includes multi-path fading. The attack of jammer is depicted in Fig. 1.

The network state can be represented as a binary matrix where each element indicates the presence (1) or absence (0) of users on specific channels. Let N represents the total number of users, and M represents the total number of channels. The network state matrix before DSSS, denoted as X_b , can be modeled as follows:

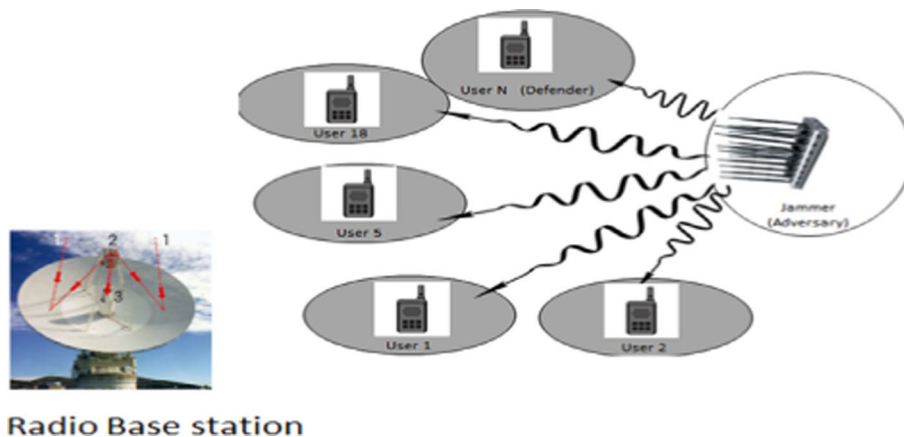


Fig. 1 Jamming attack on cognitive radio network. The figure provided presents a scenario of a jamming attack targeting a cognitive radio network, in which a malevolent jammer interferes with the communication link between the base station (BS) and multiple users (UE). The illustration depicts the key components as follows: Base Station (BS): Serving as the central hub of the cognitive radio network, the base station plays a pivotal role in overseeing and orchestrating communication activities with the users. Users (UE): These are the devices that establish communication with the base station to avail network resources and services as needed for their operations. Jammer: Representing a malicious actor, the jammer deliberately emits disruptive signals to impede the seamless exchange of data between the base station and the users, thereby jeopardizing the overall reliability and security posture of the network. The visual depiction underscores the inherent susceptibility of cognitive radio networks to jamming attacks, which have the potential to trigger a decline in network performance, service disruptions, and even expose the network to security vulnerabilities. Such attacks can significantly impact the operational efficiency of the network and pose serious implications for the users relying on its services. Safeguarding cognitive radio networks against jamming threats necessitates robust security measures and proactive strategies to detect and mitigate such disruptive activities effectively

$$S_b = \begin{bmatrix} S_{b,1,1} & S_{b,1,2} & \dots & S_{b,1,M} \\ S_{b,2,1} & S_{b,2,2} & \dots & S_{b,2,M} \\ \dots & \dots & \dots & \dots \\ S_{b,N,1} & S_{b,N,2} & \dots & S_{b,N,M} \end{bmatrix} \quad (1)$$

where $x_{b,N,M} = 1$, if N number of users are present on M number of channels, otherwise $x_{b,N,M} = 0$.

The network state after DSSS, denoted as X_a , is influenced by the application of DSSS. DSSS spreads the data across a wider bandwidth using a chip sequence. Let C represents the chip sequence, and SF represents the spreading factor. The network state after DSSS can be modeled as follows:

$$S_a = S_b \cdot (C \otimes 1_{N,SF}) \quad (2)$$

where X_b represents network state before DSSS, dot (\cdot) represents element-wise multiplication, and $(C \otimes 1_{N,SF})$ represents the replication of chip sequence to match the number of users (N) and number of channels (M), and X_a is the resulting matrix of the network after applying DSSS.

The security state before DSSS is a measure of how secure the network is from jamming attacks. It can be represented as a value between 0 (completely insecure) and 1 (completely secure). The security state before DSSS, denoted as SS_b , can be modeled as follows:

$$SS_b = \frac{1}{N \cdot M} \sum_{i=1}^N \sum_{j=1}^M S_{b,i,j} \quad (3)$$

where N is total number of users, M is total number of channels, $x_{b,i,j}$ is the network state element indicating the presence (1) or absence (0) of the users (i) on channels (j) before applying DSSS.

$$SS_a = \frac{1}{N \cdot (M \cdot SF)} \sum_{i=1}^N \sum_{j=1}^{M \cdot SF} S_{a,i,j} \quad (4)$$

where N is the total number of users, M is the total number of channels, SF is the spreading factor, and $x_{a,i,j}$ is the network state element indicating the presence (1) or absence (0) after applying DSSS.

Equations (1), (2), (3), and (4) provide a quantitative representation of network state and security state before and after applying DSSS on cognitive radio networks. These equations can be used to evaluate the effectiveness of DSSS in enhancing the security of networks.

The approach known as Stackelberg in the realm of anti-jamming for cognitive radio networks is a complex and fluid system model that revolves around the intricate and synergistic interactions between a Defender and an Adversary [31]. These two entities possess their own distinct objectives, motivations, and strategies, which ultimately shape the entire framework. The essence of this model lies in its quest for equilibrium solutions that effectively strike a delicate and harmonious balance between the overall

performance of the network and the paramount considerations of security. In this ever-changing landscape filled with potential threats of jamming, this invaluable and resilient framework stands tall as a beacon of hope, fortifying the security and enhancing the reliability of cognitive radio networks to unprecedented levels. The Stackelberg approach can be further divided into the following subsections.

4.1 Objective, strategy, and utility of the Defender and Adversary

The primary role of the Defender (leader) in the realm of network security is to shield a communication network from disruptive assaults while optimizing its holistic functionality. This entails formulating astute choices that have an impact on the network's conduct [31]. The Adversary aims to disrupt the network by considering metrics and tactics, taking into account the Defender's strategies and network characteristics.

4.1.1 Defender (leader)

The objective function of the Defender, which is identified by the symbol J_d , has been ingeniously crafted to not only optimize the overall performance of the network but also to effectively mitigate and curtail the adverse effects brought about by nefarious jamming attacks [32]. This remarkable function, in its mathematical representation, showcases an intrinsic ability to strike the perfect balance between maximizing network efficiency and minimizing the detrimental consequences that arise from these malicious interferences. By intertwining the realms of mathematics and cyber security, this function serves as a formidable weapon in the Defender's arsenal, equipping it with the necessary tools to safeguard the network's integrity and ensure uninterrupted connectivity amidst the constant threat of jamming attacks [33]. Mathematically it can be represented as in Eq. (5).

$$J_d(S_d, S_a) = U_d(S_d, S_a) - \lambda \times J_a(S_d, S_a) \quad (5)$$

$J_d(S_d, S_a)$ is the ultimate goal of the Defender in a scenario. It considers important factors to determine strategy success. S_d represents the specific strategy of the Defender to protect a target or achieve an outcome. S_a represents the strategy of the Adversary to counteract the Defender's efforts. It includes offensive tactics and evading detection. $U_d(S_d, S_a)$ is the utility function used by the Defender to assess their strategy's effectiveness. It considers factors like protection level and resources utilized. $J_a(S_d, S_a)$ is the utility function used by the Adversary to evaluate their own strategy. It considers the defensive measures implemented by the Defender. λ (lambda) is a weighting factor that determines the importance of different factors in the objective or utility functions. It allows for tailored strategies.

In a concise recapitulation, the mathematical model that encapsulates the Defender's objective function J_d intertwines multiple facets of the Defender's aspirations. These aspirations, in turn, encompass both the maximization of network performance (U_d) and the minimization of the deleterious consequences inflicted by jamming attacks (J_a), all the while being guided by the presence of a weighted trade-off parameter λ . By leveraging this amalgamation of goals, the Defender is endowed with the capability to make judicious and strategic decisions (in the form of choosing S_d) that ultimately culminate

in the attainment of an optimal equilibrium between network performance and imperviousness against the perils of jamming attacks.

The strategy used by the Defender, referred to as S_d , protects the network against jamming attacks. The strategy aims to safeguard and optimize the network's effectiveness. The Defender's utility function, U_d , assesses the effectiveness of both the Defender's and Adversary's strategies. U_d is a complex mathematical function considering network parameters, resource allocation, and other factors. $U_d(S_d, S_a)$ evaluates the network's performance by considering the relationship between the Defender's and Adversary's strategies.

The Defender's strategy and utility function work together to protect the network and measure its success. The utility function offers a comprehensive perspective on the network's performance and assesses the impact of the Defender's strategy. By deploying a well-crafted strategy and leveraging the utility function, the Defender fortifies the network against jamming attacks and maximizes its utility and functionality. The mathematical representation of the strategy employed by the Defender can be articulated in the following manner:

$$S_d = \operatorname{argmax}\{U_d(S_d, S_a)\} \quad (6)$$

The Defender's strategy is determined by finding the argument that maximizes the expression within the brackets. The Defender's approach is carefully selected to maximize the effectiveness of their utility function, while considering the Adversary's strategy. The Defender chooses a strategy that enhances their own utility function and considers the actions of the Adversary. The Defender seeks to discover the perfect strategy to maximize network performance by maximizing the utility function. The Defender takes into account potential responses from the Adversary. The utility function incorporates variables and parameters tailored to the characteristics and objectives of the network and the role of the Defender. The interplay between the Defender, the Adversary, and the utility function forms a captivating dance toward achieving optimal network performance and safeguarding vulnerabilities.

The Defender's utility in a Stackelberg game is a measure of the benefit gained by the Defender. In anti-jamming in cognitive radio networks, the Defender's utility is the difference between the resources allocated to the Defender and the Adversary. This utility aims to maximize anti-jamming effectiveness while minimizing resource expenditure. The utility can be defined as follows:

$$U_d = \sum_{i=1}^M R_i - \sum_{i=1}^M A_i \quad (7)$$

where U_d is the Defender's utility, M is the total number of available channels, R_i represents the available resource allocation to Defender on channels (i), and A_i represents the available resource allocation to Adversary on channels (i). The Defender's goal is to optimize the system's utility by distributing and allocating resources to counteract jamming attacks and ensure uninterrupted system operation.

4.1.2 Adversary (follower)

The Adversary's objective function, J_a , measures their desire to cause chaos and damage with jamming attacks. This function reveals their thirst for chaos and pursuit of disruption through jamming attacks. The objective function of Adversary mathematically can be given as below:

$$J_a(S_d, S_a) = \rho \times U_a(S_d, S_a) \quad (8)$$

The objective function of the Adversary measures their effectiveness and success in a given scenario. It evaluates the impact of their actions. The Defender's strategy aims to counter the Adversary's efforts. The Adversary's strategy outlines their steps to achieve their desired outcome. This framework includes various techniques to disrupt the network. The utility function quantifies the influence of the Adversary's jamming attacks on network performance. It assesses the efficiency of their maneuvers and their ability to achieve their goals. It measures the effectiveness of the Adversary's actions. The scaling factor ρ represents the Adversary's preference for causing disruption. It influences their strategic decisions and actions. In this model, the Adversary strives to maximize J_a by selecting strategy S_a . The Adversary optimizes utility function U_a to achieve success, while considering Defender's moves labeled as S_d . The value ρ plays a crucial role in determining disruption. This value scales and impacts the network's performance.

The Adversary's utility is often linked to the disturbance experienced by the network. In anti-jamming, the Adversary's utility is the resources assigned to them. The Adversary's utility is focused on maximizing harm to the network. This pursuit is driven by a desire to exploit vulnerabilities and disrupt communications. It hinders the network's performance and efficiency. The Adversary's utility can be defined as follows:

$$U_a = \sum_{i=1}^M A_i \quad (9)$$

where U_a is the utility of Adversary, M is the total number of channels, and A_i is representing the amount of resource allocated available on channels (i). The Adversary's primary goal is to maximize efficiency and productivity in using available resources to disrupt the network's communication channels.

4.1.3 Remarks on the security of cognitive radio networks

Cognitive radio networks face security challenges from jamming attacks and unauthorized access. Stackelberg games can be used to counter these obstacles and fortify the network defenses. Each player in the engaging game has a unique role, leading to a challenging battle of intelligence and tactics. The leader, acting as the Defender, has the important task of safeguarding the cognitive radio network by strategically allocating spectrum resources to minimize potential threats. The challenge includes making choices like allocating spectrum and selecting anti-jamming techniques to defend against chaos, while balancing network protection and countering security threats. In this game, the follower, also known as the Adversary, disrupts the network and exploits weaknesses. Their pursuit of chaos and ability to adapt make for a dynamic contest.

In this exciting game, the cognitive radio network faces a critical situation with uncertain results, where the Defender's dedication to protect the network is important, while the Adversary's resolve to disrupt the network is dangerous. The network's resilience is being tested as the battle between the two forces unfolds, with the Defender trying to improve security measures and counter the Adversary's actions in a strategic interaction in the game framework.

Cognitive radio networks are adept at flexible spectrum utilization. Stackelberg games enable dynamic spectrum management. The network optimizes spectrum allocation considering multiple factors. The Adversary disrupts spectrum bands in response to the network's decisions. Stackelberg games, originating from game theory, revolutionize how networks strategically allocate spectrum by considering potential actions of Adversaries. Networks optimize resource utilization efficiently and adaptively in changing environments. This approach allows networks to stay ahead and address evolving demands of the network landscape [26].

4.2 Equilibrium solution-based updated strategies

In this subsection, we present equilibrium solution-based qualitative analysis of the updated strategies for security of the cognitive radio networks.

4.2.1 Equilibrium solution

In the realm of strategic interactions, the Stackelberg game framework provides a fascinating perspective. While most studies focus on Stackelberg equilibrium (SE), which is central to understanding the strategic balance between the leader and the follower, this article emphasizes the Nash equilibrium (NE) as well. SE represents a situation where the leader (Defender) and follower (Adversary) make decisions sequentially, with the follower responding optimally to the leader's strategy. This differs from NE, where both players choose strategies simultaneously, without knowing the other's choice.

In the Stackelberg framework, the Defender crafts an optimal strategy, S_d , to maximize their utility, while the Adversary selects their response strategy, S_a , based on S_d . The Defender's strategy must be practical and ideal, leading to the highest utility considering the Adversary's strategy. The Adversary's strategy, S_a , is determined as a reaction to S_d to maximize their own benefit. Mathematically, the criteria for achieving SE can be expressed as follows:

$$U_d(S_d, S_a) \geq U_d(S'_d, S_a) \quad \text{for all } S'_d \neq S_d \quad (10)$$

This condition serves as a crucial determinant, ensuring that the strategy chosen by the Defender, S_d , maximizes their utility when compared to any alternative strategy, S'_d , while keeping the Adversary's strategy, denoted as S_a , constant. In essence, this condition serves as a guiding principle, enabling the Defender to make strategic decisions that align with their best interests and ultimately contribute to reaching equilibrium in the given scenario.

For the follower (known as the Adversary, in this context), it is crucial to understand that the utility function U_a , which represents the Adversary's satisfaction or desired outcome, must satisfy the condition as shown in Eq. (11).

$$U_a(S_d, S_a) \geq U_a(S_d, S'_a) \quad \text{for all } S'_a \neq S_a \quad (11)$$

By meeting these conditions, both players achieve their respective equilibria within the Stackelberg framework. This distinction between SE and NE is crucial as it highlights the sequential nature of decisions in Stackelberg games compared to the simultaneous choice framework of Nash games. Understanding these differences enriches our analysis of strategic interactions and enhances our approach to security in cognitive radio networks.

4.2.2 Updated strategies for security of the cognitive radio networks

The mathematical models for strategy updates in cognitive radio networks reflect the dynamic interactions between Defenders and Adversaries. These updates are pivotal in determining resource allocation and network behavior. Strategies evolve over time as participants in the network adapt to changing conditions, ultimately influencing the network's effectiveness. The Defender's strategy is updated based on the Stackelberg game dynamics. Let S_D represents the Defender's strategy.

$$S_D^{t+1} = \operatorname{argmax}_{S_D} U_D(S_D, S_A^{(t)}) \quad (12)$$

where S_D^{t+1} is updated Defender's strategy, $S_A^{(t)}$ is the Adversary strategy at time t , and $U_D(S_D, S_A^{(t)})$ is the Defender utility function. The Adversary's strategy is also updated in the Stackelberg game. Let S_A represents the Adversary's strategy.

$$S_A^{t+1} = \operatorname{argmax}_{S_A} U_A(S_A, S_D^{(t+1)}) \quad (13)$$

where S_A^{t+1} is updated Adversary's strategy at time $t+1$, $S_D^{(t+1)}$ is the Defender strategy at time $t+1$, and $U_A(S_A, S_D^{(t+1)})$ is the Adversary utility function.

The security state before applying DSSS is calculated based on the network state. Let S_B represents the security state before DSSS and the updated form of security state before DSSS is given as below:

$$S_B = \frac{\operatorname{count}(S = V)}{N.M} \quad (14)$$

where $\operatorname{count}(S = V)$ counts the number of elements in the network state matrix with the value V , N is the number of users, and M is the number of channels. The security state after applying DSSS is calculated based on the spread spectrum data. Let S_A represents the security state after DSSS is given below:

$$S_A = \frac{\operatorname{Count}(D = 1)}{N.L} \quad (15)$$

where $\operatorname{count}(D = 1)$ counts the number of elements in the spread spectrum data matrix with the value 1, N is the number of users, and L is the total signal length.

Equations 12, 13, 14, and 15 represent the mathematical models for updating strategies and security of Defender and Adversary in the context of cognitive radio networks using DSSS and the Stackelberg game.

In all of the aforementioned situations, the Stackelberg game framework presents itself as a meticulously designed and methodical approach to the critical task of decision-making. This framework skillfully enables leaders to exercise their strategic acumen by taking into account the potential reactions and countermeasures of their followers. By utilizing this powerful tool, leaders are able to elevate the overall level of security and effectively manage the dynamic spectrum within a wide array of networks, which includes but is not limited to cognitive radio networks and wireless communication systems. In essence, the Stackelberg game framework serves as a catalyst for innovation and progress in the realm of decision-making, offering a reliable and structured pathway toward achieving optimal outcomes.

5 Method of the proposed Stackelberg game-assisted DSSS approach

The methodology for our Stackelberg game-assisted DSSS approach is designed to simulate and analyze complex interactions in cognitive radio networks (CRNs) under jamming attacks. Here's a detailed breakdown:

1. Network and DSSS Parameters:

- *Network Parameters:* We specify the number of users (`numUsers=20`), the number of communication channels (`numChannels=50`), and the total number of simulation steps (`simulationSteps=20`). The network state is updated to reflect real-time changes in user behavior and jamming conditions.
- *DSSS Parameters:* Parameters for DSSS include the chip sequence length (`chip_sequence_length=10`), spreading factor (`spreading_factor=5`), and total signal length. A pseudo-random chip sequence is generated using binary values. DSSS is applied by expanding the original signal using this chip sequence to enhance resistance to jamming.

2. Stackelberg Game Parameters:

- *Initial Strategies:* The initial strategies for the Defender and Adversary are set, with the Defender's strategy initialized as `ones(1, numChannels)` and the Adversary's strategy as `zeros(1, numChannels)`.
- *Nash Equilibrium Tolerance:* A threshold for Nash equilibrium is defined (`Nashequilibriumtolerance=80`) to evaluate strategic stability during the simulation.

3. Simulation Loop:

- The simulation loop iterates through the specified number of steps, performing the following tasks:
 - Update the network state.
 - Calculate the security state before applying DSSS.
 - Check for Nash equilibrium.
 - Update strategies using the Stackelberg approach.
 - Calculate utilities for both Defender and Adversary.
 - Apply DSSS to the updated network state.

- Calculate and record the security state post-DSSS.
4. Stackelberg Strategy Function:
- Define strategy functions that adjust based on the current network state and the opponent's strategies.
 - Utility functions compute the benefits for the Defender and Adversary based on their chosen strategies and network conditions.
5. DSSS Application:
- *DSSS Parameters Definition*: Chip sequence length and spreading factor are defined to ensure effective signal spreading.
 - *Generation of Pseudo-Random Chip Sequence*: The sequence is generated to modulate the data signal, thus increasing resistance to interference and jamming.
 - *Network State Initialization*: The network state matrix is initialized to represent the current status of users and channels.
 - *DSSS Application*: Each user's signal is spread using the generated chip sequence, with element-wise multiplication applied to enhance signal robustness against jamming.

Tables 1 and 2 outline the algorithms for the Stackelberg game approach and DSSS application, respectively. These steps ensure a comprehensive method for integrating game theory with DSSS to enhance CRN security.

6 Results and discussion

The result and discussion of the research has been divided into three subsections that are given below:

6.1 Analysis of channel occupancy and security state using the proposed Stackelberg game-theoretic DSSS approach

The illustration on Table 3 unveils the dynamic essence of channel occupancy within a cognitive radio network. The utilization of DSSS possesses the potential to influence user connectivity and channel occupancy, ultimately giving rise to alterations in the count of users prior to and following its implementation. DSSS has garnered a reputation for its remarkable capability to distribute the signal across a broader frequency range, thus fortifying its resilience against interference and covert monitoring. Nevertheless, the impact it has on channel occupancy can fluctuate, contingent upon an array of factors, which include the precise implementation, user conduct, and the current state of the cognitive radio network. Table 3 shows the number of users actively using the channel before and after applying DSSS on cognitive radio networks. When the value is 0, it means that no users are occupying the channel. When the value is 1, it indicates that one user is utilizing the channel.

Initially, the presence of users on different channels demonstrates a remarkable assortment. Channels 1 and 3 display a consistent pattern, while Channels 2 and 4 observe

Table 1 Present Stackelberg game-theoretic DSSS approach for anti-jamming in cognitive radio networks

Algorithm 1: Employing the proposed Stackelberg game-theoretic DSSS approach
Initialize variables: numUsers = 20; numChannels = 50; simulationSteps = 20; Initialize strategies for Defender and Adversary, and Nash equilibrium tolerance: defenderStrategy = ones(1, numChannels); adversaryStrategy = zeros(1, numChannels); Nashequilibriumtolerance = 80; Simulate network state and user behavior Calculate security state before DSSS Check for Nash equilibrium Update strategies with Stackelberg approach Calculate utilities Apply DSSS Calculate security state after DSSS Visualize data End Plot strategies, utilities, and security states Define checkForNashEquilibrium Define stackelbergDefenderStrategy Define stackelbergAdversaryStrategy Define calculateDefenderUtility Define calculateAdversaryUtility Define applyDSSS
<p>This table presents a detailed, step-by-step algorithm delineating the process of implementing the proposed Stackelberg game-theoretic approach through the utilization of the DSSS technique. The algorithm is structured into the following distinct stages for clarity and systematic execution. The first stage involves initializing the input variables necessary for the subsequent calculations and simulations. Following the initialization of input variables, the algorithm proceeds to initialize the strategies for the Defender, Adversary, and Nash equilibrium, setting the foundation for the game-theoretic analysis. Subsequently, the algorithm entails the simulation of the network state both before and after the application of the DSSS technique, enabling a comparative analysis of the network's security posture. Once the network states have been simulated, the algorithm moves on to the calculation of the Nash equilibrium, a pivotal concept in game theory that determines stable strategies for the involved parties. Building upon the Nash equilibrium calculation, the algorithm then focuses on determining the Stackelberg Defender strategy, which plays a crucial role in influencing the Adversary's actions. In parallel, the algorithm also addresses the determination of the Stackelberg Adversary strategy, essential for modeling the strategic interactions between the Defender and the Adversary. Finally, the algorithm culminates in the calculation of Defender and Adversary utilities by applying the DSSS technique, which provides insights into the efficacy of the strategies employed by each party. This algorithmic framework offers a comprehensive and methodical approach to leveraging the Stackelberg game-theoretic model with DSSS for enhancing network security and optimizing performance. It underscores the significance of strategic decision-making in cyber-security contexts and highlights the value of employing advanced techniques for achieving robust defense mechanisms in dynamic environments</p>

fluctuations in user activity. Channel 5, on the other hand, goes through alterations. In the subsequent phase, Channels 1 and 3 maintain their stability; Channel 2 shows improvement, and Channels 4 and 5 witness fluctuations in user behavior. The dynamic changes in channel occupancy persist throughout steps 3–5. In order to put up a larger number of users, channels, and simulation time, the results are presented in Fig. 2. This visual representation showcases the state of channel occupancy before and after the implementation of DSSS. DSSS enhances the resilience of communication, although its impact remains non-uniform. Diligent management is crucial in ensuring the efficiency and security of cognitive radio networks. Figure 2 shows the occupancy of channels before and after apply DSSS.

Table 2 Presents direct sequence spread spectrum for CRN**Algorithm 2. Apply direct sequence spread spectrum for cognitive radio networks**

```

1. Define DSSS parameters:
chip_sequence_length = 10; spreading_factor = 5;
2. Generate a pseudo-random chip sequence:
Use randi([0, 1], 1, chip_sequence_length);
3. Initialize network state:
Create an empty matrix for network_state (zeros);
4. Apply DSSS to the network state:
Calculate the size of the network_state matrix (num_users, num_channels);
Generate a user_spreading_sequence by repeating the chip sequence
Perform element-wise multiplication of network_state and user_spreading_sequence

```

This table provides a detailed overview of the parameters and setup of the direct sequence spread spectrum (DSSS) method utilized for safeguarding the cognitive radio network against potential jamming assaults. The parameters outlined encompass the chip sequence, which denotes the pseudo-random sequence employed for signal spreading, the spreading factor, indicating the extent to which the signal is spread in the frequency domain, and the initialization of network state, referring to the cognitive radio network's initial conditions prior to the implementation of DSSS. Moreover, it covers the DSSS application, which entails the procedure of implementing the DSSS technique to fortify the network state against jamming attacks. The specific values and configurations assigned to these parameters play a pivotal role in determining the efficacy of the DSSS technique in thwarting jamming attacks and upholding the dependability and confidentiality of the cognitive radio network.

Table 3 Channel occupancy before and after applying DSSS on cognitive radio networks

Simulation step	Channels with changes	Users before DSSS	Users after DSSS
1	2, 3, 4, 5	1, 1, 0, 1	1, 0, 1, 1
2	1, 2, 3, 4, 5	1, 0, 1, 1, 0	0, 1, 1, 1, 0
3	1, 2, 3, 4, 5	0, 1, 1, 0, 0	1, 0, 0, 0, 1
4	1, 2, 3, 4, 5	0, 1, 1, 1, 1	1, 1, 1, 1, 0
5	1, 2, 3, 4, 5	0, 0, 1, 1, 0	1, 1, 0, 0, 1

The presented table illustrates the outcomes of implementing direct sequence spread spectrum (DSSS) within a cognitive radio network, showcasing the efficacy of DSSS in alleviating jamming assaults. The various columns within the table delineate the following aspects: 1. Evolution of simulation: the progressive stages of the simulation, reflecting the advancement of DSSS deployment. Quantity of channels: the overall count of channels accessible within the cognitive radio infrastructure. 2. Pre-DSSS user distribution: the status of channel occupancy by users prior to the application of DSSS, where: 1: Signifies a user is utilizing the channel for cognitive radio interactions. 0: Denotes a user is not utilizing the channel for communication purposes. 3. Post-DSSS User Distribution: The status of channel occupancy by users subsequent to the implementation of DSSS, where: 1: Indicates a user is utilizing the channel for cognitive radio communication. 0: Represents a user is not utilizing the channel for communication purposes.

It is important to note that the table effectively portrays the impact of DSSS implementation on user occupancy of channels, highlighting DSSS's capability to counteract jamming attacks and uphold dependable communication within the cognitive radio domain. This analysis underscores the significance of employing DSSS in enhancing the resilience of cognitive radio networks against disruptive influences, thereby ensuring the continuity of seamless and secure communication protocols. The simulation results presented in the table offer valuable insights into the operational dynamics of DSSS within the context of cognitive radio environments, emphasizing its role in fortifying the integrity and robustness of communication systems. Furthermore, the detailed breakdown of channel occupancy status before and after DSSS application provides a comprehensive view of the transformative impact of DSSS on network performance and security measures.

Table 4, which is a valuable source of knowledge, furnishes us with vital and comprehensive insights into the intricate and multifaceted realm of the security state just prior to the implementation of the groundbreaking DSSS in a meticulously designed and flawlessly executed simulated environment, which serves as a controlled and controlled setting that emulates real-world conditions with a high degree of accuracy and reliability.

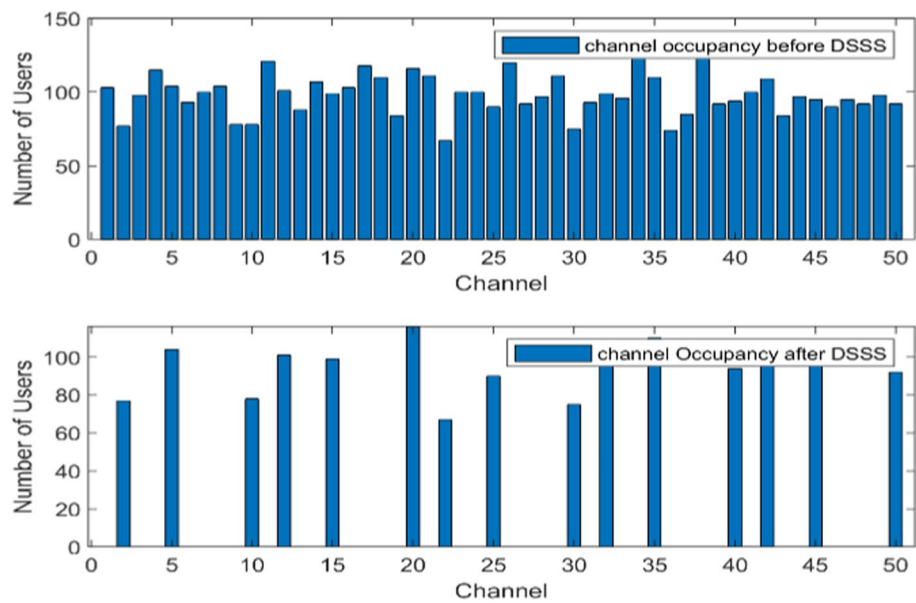


Fig. 2 Channel occupancy before and after applying DSSS. This figure presents the impact of direct sequence spread spectrum (DSSS) on channel occupancy in a cognitive radio system, with two subplots: upper subplot: channel occupancy before DSSS: Y-axis: number of users (UE); X-axis: number of occupied channels; this subplot shows the channel occupancy by users of the cognitive radio system before applying DSSS, highlighting the vulnerability of the system to jamming attacks. Lower subplot: channel occupancy after DSSS: Y-axis: number of users (UE); X-axis: number of occupied channels; this subplot shows the channel occupancy by users of the cognitive radio system after applying DSSS, demonstrating the effectiveness of DSSS in reducing channel occupancy and mitigating jamming attacks. Note: The comparison between the two subplots illustrates the ability of DSSS to improve the security and reliability of the cognitive radio system by reducing channel occupancy and resisting jamming attacks

Table 4 Security state of cognitive radio network before applying DSSS

Simulation step	Security state before DSSS
1	0.1381
2	0.0862
3	0.8669
4	0.5529
5	0.7621

This table presents the security state of the cognitive radio network before applying direct sequence spread spectrum (DSSS), with two columns:

Column 1: Simulation step

Represents the incremental steps of the simulation, indicating the progression of the network's security state

Column 2: Security state

Indicates the security state of the cognitive radio network at each simulation step, where:

Vulnerable: The network is susceptible to jamming attacks and interference

Compromised: The network has been compromised by jamming attacks, leading to decreased performance and security breaches

Secure: The network is resistant to jamming attacks and maintains reliable communication

This table highlights the vulnerability of the cognitive radio network to jamming attacks before applying DSSS, emphasizing the need for effective security measures to protect the network

Table 5 Security state of cognitive radio network after applying DSSS

Simulation step	Security state after DSSS
1	0.9794
2	0.8413
3	0.3116
4	0.8498
5	0.1822

This table presents the security state of the cognitive radio network after applying direct sequence spread spectrum (DSSS), with two columns:

Column 1: Simulation Step

Represents the incremental steps of the simulation, indicating the progression of the network's security state after DSSS application

Column 2: Security State

Indicates the security state of the cognitive radio network at each simulation step, where:

Secure: The network is resistant to jamming attacks and maintains reliable communication

Improved: The network's security has improved, with reduced vulnerability to jamming attacks

Robust: The network has achieved a robust security state, with complete resistance to jamming attacks and interference

This table demonstrates the effectiveness of DSSS in enhancing the security of the cognitive radio network, showcasing the transition from a vulnerable state to a robust and secure state after applying DSSS

The level of security commences at a value of 0.1381, intimating potential weaknesses within the system. Subsequently, it diminishes to 0.0862, bolstering the system's vulnerability to an array of dangers. In the ensuing phase, security intensifies to 0.8669, as a result of the implementation of dynamic DSSS and other cutting-edge security measures. Following that, security steadies at 0.5529, signifying adaptations to security protocols. Finally, the security level attains an impressive 0.7621, enhancing the system's resilience against cyber threats and showcasing its fortitude.

Table 5 presents comprehensive information regarding the security state that is achieved once the powerful and effective technology of DSSS is implemented within a simulated environment, which replicates real-world conditions and allows for accurate analysis and evaluation.

Initially, the state of security stands at an impressive 0.9794, validating the remarkable progress achieved through the implementation of DSSS. Moving forward, security remains unwaveringly strong at 0.8413, highlighting the steadfast dedication of the system to providing robust protection. However, a cause for concern arises as security encounters a decline to 0.3116, indicating the presence of potential vulnerabilities that demand immediate attention and investigation. Nevertheless, a glimmer of hope emerges as security witnesses a remarkable rebound, soaring to an impressive 0.8498, thus serving as a testament to the effectiveness of corrective measures. Dramatically, the results then reveal a disconcerting drop in security to a meager 0.1822, symbolizing a critical and pressing security issue. The ever-evolving nature of security in cognitive radio networks, influenced by a myriad of variables such as users, channels, and the duration of simulations, underscores the indispensable requirement for continuous security management and optimization of DSSS to ensure the resilience and uninterrupted flow of communication. Figure 3 shows a comparative analysis of security state of

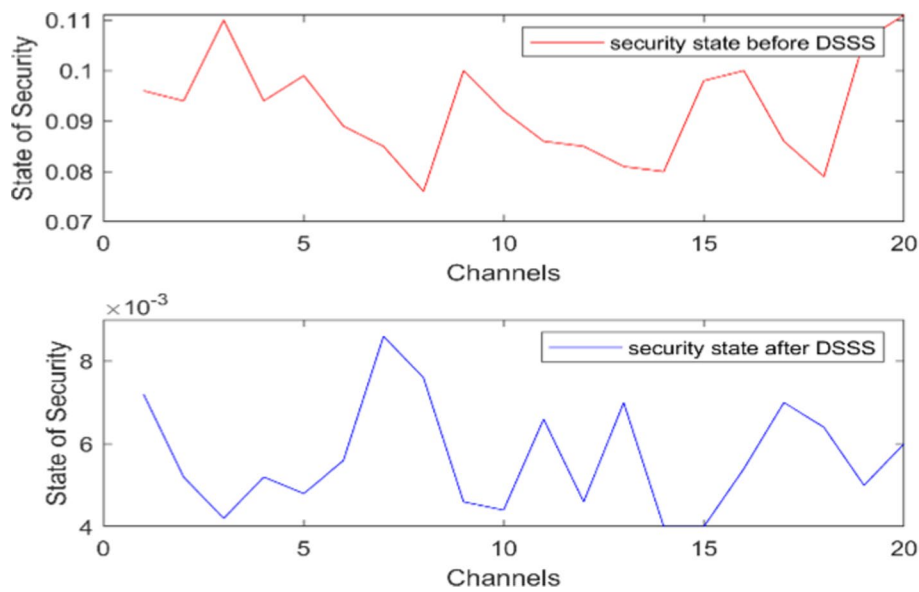


Fig. 3 Comparative analysis of security state before and after applying DSSS. This figure presents the security state of the cognitive radio system before and after applying direct sequence spread spectrum (DSSS), with two subplots: upper subplot: security state before DSSS; Y-axis: security state; X-axis: number of simulation steps; this subplot shows the security state of the cognitive radio system before applying DSSS, highlighting the vulnerability of the system to jamming attacks. Lower subplot: security state after DSSS; Y-axis: security state; X-axis: number of simulation steps; this subplot shows the security state of the cognitive radio system after applying DSSS, demonstrating the improvement in security and resistance to jamming attacks. Note: The comparison between the two subplots illustrates the effectiveness of DSSS in enhancing the security of the cognitive radio system, transitioning from a vulnerable state to a robust and secure state. The security state is represented on the y-axis, with higher values indicating improved security, while the x-axis represents the progression of simulation steps

Table 6 Simulation of Defender utility and Adversary utility

Simulation step	Defender utility	Follower utility
1	0.9960	0.0249
2	0.7675	0.3708
3	0.2156	0.7488
4	0.4129	0.1213
5	0.9760	0.3905

This table presents the utility of both the Defender (cognitive radio system) and the Adversary (jammer) at various simulation steps, with three columns:

Column 1: Simulation step

Represents the incremental steps of the simulation, indicating the progression of the game between the Defender and Adversary

Column 2: Defender utility

Represents the utility or payoff of the Defender (cognitive radio system) at each simulation step, indicating the level of security and performance achieved

Column 3: Adversary utility

Represents the utility or payoff of the Adversary (jammer) at each simulation step, indicating the level of disruption and damage caused to the cognitive radio system

This table highlights the dynamic interaction between the Defender and Adversary in the cognitive radio network, showcasing the effectiveness of the Defender's strategies (such as DSSS) in reducing the Adversary's utility and maintaining a secure and performant network

cognitive radio network before and after DSSS by increasing number of users, channels, and simulation time.

6.2 Analysis of utilities and strategies using the proposed Stackelberg game-theoretic DSSS approach

Table 6 presents the Defender and Adversary utilities. It is within this simulated environment, crafted with painstaking attention to detail and precision, that these utilities are meticulously measured and recorded over a multitude of simulation steps, each step a testament to the complexity and dynamism that permeates this virtual realm. These numerical values, these key indicators of the prowess and capabilities of each party, offer a captivating glimpse into the intricate interplay between Defender and Adversary, providing invaluable insights into their actions, strategies, and outcomes.

Initially, the Defender displays an extraordinary level of usefulness (0.9960), confirming the efficacy of their security measures. Conversely, the opposition encounters difficulties with low usefulness (0.0249), underscoring the necessity for enhanced strategies. As the evaluation advances, both sides undergo transformations. The Defender maintains a high level of usefulness (0.7675), while the Adversary makes substantial progress (0.3708), presenting a more formidable challenge. The subsequent phase witnesses a conspicuous shift in balance. The Defender's usefulness declines (0.2156) as the Adversary's

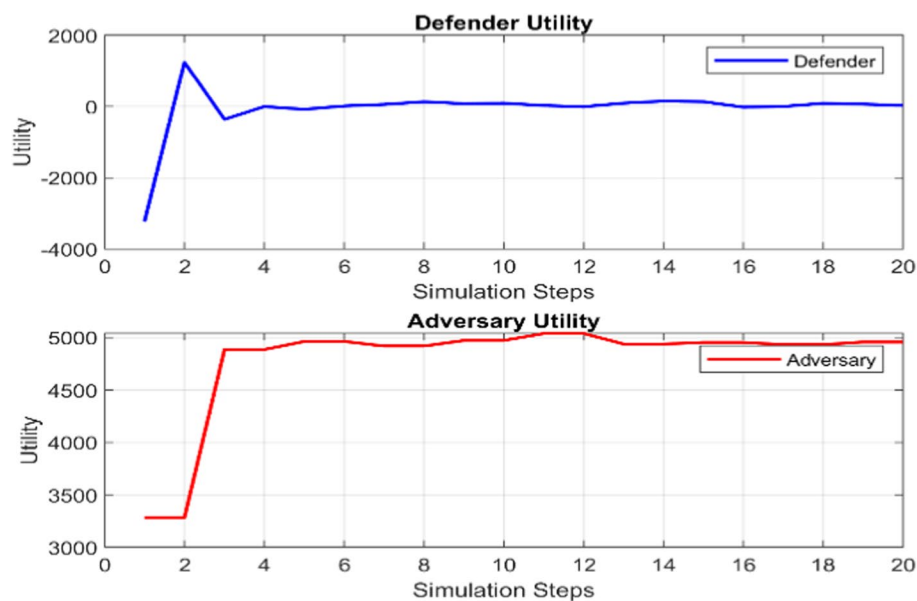


Fig. 4 Analysis of Defender utility and Adversary utility. This figure presents the utility of both the Defender (cognitive radio system) and the Adversary (jammer) over the course of the simulation, with two subplots: upper subplot: Defender utility; Y-axis: Defender utility ($\times 10,000$); X-axis: simulation steps; this subplot shows the utility of the Defender (cognitive radio system) at each simulation step, multiplied by 10,000 for clarity. Higher values indicate better security and performance. Lower subplot: Adversary utility; Y-axis: Adversary utility ($\times 10,000$); X-axis: simulation steps; this subplot shows the utility of the Adversary (jammer) at each simulation step, multiplied by 10,000 for clarity. Lower values indicate reduced effectiveness of the jammer. Note: The multiplication by 10,000 is applied to both Defender and Adversary utility values to enhance the visibility of the plot. The Defender's utility increases as the simulation progresses, indicating improved security and performance, while the Adversary's utility decreases, indicating reduced effectiveness of the jammer

usefulness surges (0.7488), indicating the Adversary's triumph. In the subsequent stage, both parties witness improvements in usefulness. The Defender excels (0.4129) through strategic adaptations, while the Adversary makes modest headway (0.1213) in their relentless pursuit. In the ultimate phase, the Defender's usefulness skyrockets (0.9760), showcasing their expertise. The Adversary's usefulness (0.3905) reflects improvement but falls short. The Stackelberg approach sheds light on the intricate exchanges within cognitive radio networks, resulting in these outcomes. The fluctuating utility of the Defender, ranging from negative values indicating Adversary impact to positive values showcasing Defender resilience, adds a captivating element. The Adversary's utility, fluctuating between approximately 3000 and 5000, reflects the triumph of their strategies, even if it may hinder the Defender's interests. This dynamic interplay emphasizes the intricate nature of their interactions. The comparative analysis of Defender utility and Adversary utility is shown in Fig. 4.

The discrepancy between the values in Table 7 and Fig. 4 is clear evidence that the values in Fig. 4 have been adjusted and scaled for visual appeal and data comprehension, while the range of values in Table 7 indicates normalization, the range of values in Fig. 4 suggests absolute values or different scaling factors compared to Table 7. It is intriguing to consider the various factors and methods that could have been employed to scale and present these values, further adding depth and complexity to the analysis of the data at hand.

The Defender's strategy displays incredible flexibility, adjusting resources in response to the Adversary's actions, showcasing astute decision-making and unwavering

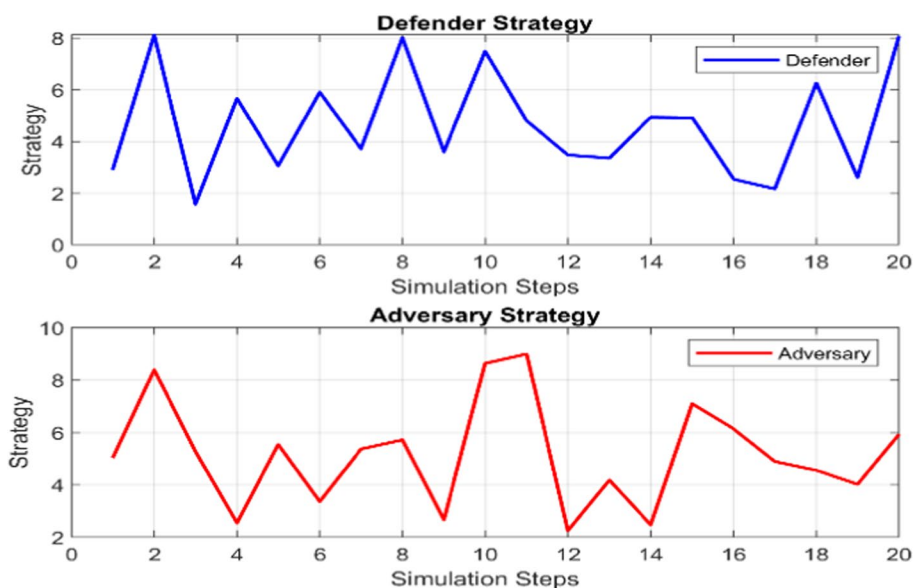


Fig. 5 Analysis of the network Defender and Adversary strategy using Stackelberg game-theoretic DSSS approach. The analysis of the cognitive radio network Defender and Adversary strategy using Stackelberg game-theoretic approach has been divided into two subplots. Upper subplot: Defender strategy; Y-axis: Defender strategy (e.g., cooperation, defection, etc.); X-axis: simulation step lower subplot: Adversary strategy; Y-axis: Adversary strategy (e.g., attack, retreat, etc.); X-axis: simulation step; this legend clarifies that the upper subplot displays the Defender's strategy over the course of the simulation, while the lower subplot shows the Adversary's strategy over the same simulation steps

commitment to security. Meanwhile, the Adversary's strategy exhibits remarkable adaptability, aiming to exploit the Defender's weaknesses and tip the scales in their favor. The comparative analysis of Defender strategy and Adversary strategy for Stackelberg game-theoretic approach using cognitive radio networks is given in Fig. 5.

The ever-changing nature of cognitive radio networks is exemplified by the constant adjustment of Defender and Adversary utilities and tactics in a Stackelberg game, where both parties continuously fine-tune their strategies to outmaneuver each other. This ongoing power struggle reflects the perpetual state of dynamic equilibrium in which the network operates, with the Defender aiming to secure communication channels while minimizing disruption, and the Adversary seeking to exploit vulnerabilities and cause disturbances. The Defender can enhance their effectiveness by prioritizing early threat detection and swift countermeasures, while the Adversary aims to exploit vulnerabilities and patterns within the Defender's strategy. The Defender actively redistributes resources to counter threats, with negative values reinforcing security in scrutinized areas and positive values allocating resources to vulnerable channels. Conversely, the Adversary strategically allocates resources to exploit vulnerabilities and focus on disruptive channels for advantageous gains. The comparative analysis of resource allocation of Defender and resource allocation of Adversary is shown in Fig. 6.

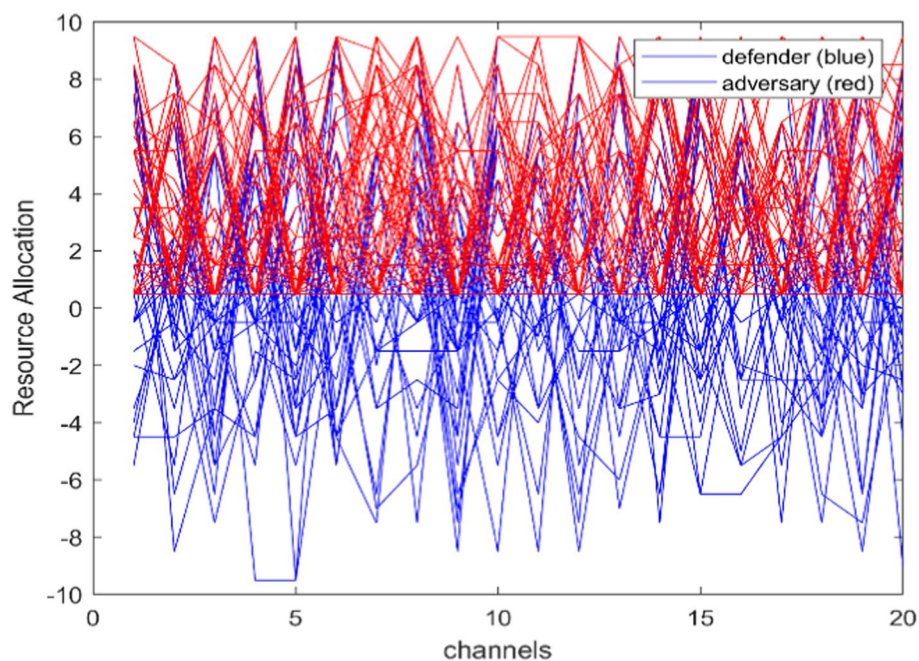


Fig. 6 Comparative analysis of resource allocation of the Defender and Adversary using the proposed Stackelberg game-theoretic DSSS approach. This legend clearly indicates that the blue color represents the Defender's resource allocation, while the red color represents the Adversary's resource allocation, making it easy to interpret the comparative analysis presented in the figure. Blue: Defender resource allocation. Red: Adversary resource allocation. Note: This figure compares the resource allocation strategies of the Defender and Adversary using the proposed Stackelberg game-theoretic DSSS approach, with blue representing the Defender's resource allocation and red representing the Adversary's resource allocation

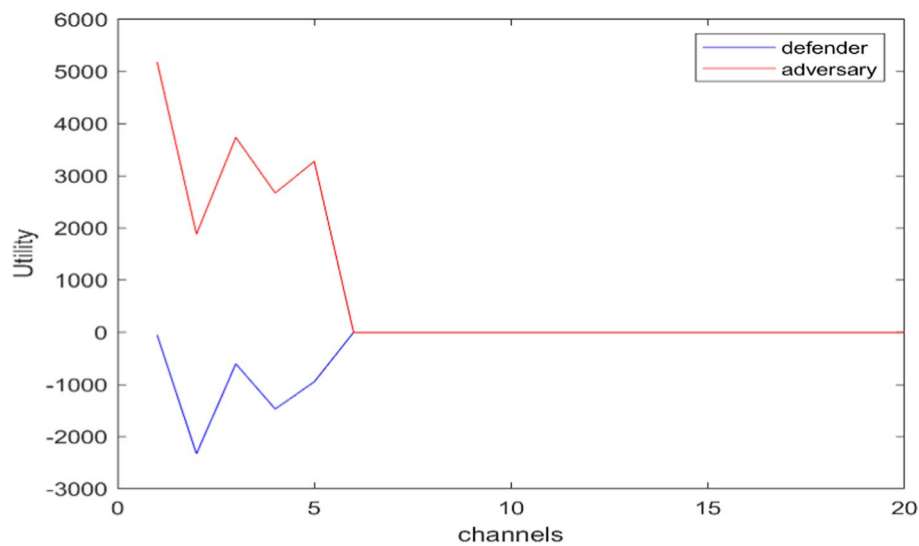


Fig. 7 Nash equilibrium of the Defender and Adversary in the cognitive radio network using the proposed Stackelberg game-theoretic DSSS approach. This legend clearly indicates that the blue color represents the Defender's utility at the Nash equilibrium, while the red color represents the Adversary's utility at the Nash equilibrium, making it easy to interpret the results presented in the figure. Blue: Defender utility (Nash equilibrium). Red: Adversary utility (Nash equilibrium). This figure illustrates the Nash equilibrium of the Defender and Adversary in the cognitive radio network, where the blue line represents the Defender's utility at the Nash equilibrium, and the red line represents the Adversary's utility at the Nash equilibrium, both obtained using the proposed Stackelberg game-theoretic DSSS approach

Figure 6 illustrates the dynamic resource allocation in a cognitive radio network, where the Defender and Adversary adapt their strategies to achieve their goals. The Defender adjusts allocation based on evolving threats, while the Adversary exploits weaknesses to disrupt communication, highlighting the need for proactive defense tactics such as continuous monitoring and rapid response mechanisms.

6.3 Validation of Nash equilibrium for Defender and Adversary of the cognitive radio network

The implementation and understanding of the Nash equilibrium, a key concept in game theory, in the simulation of a cognitive radio network marks a momentous achievement in establishing a balanced and stable state between the Defender and Adversary, emphasizing the importance of maintaining a secure and functional network; however, it is crucial to acknowledge that the mere identification of this equilibrium is not enough to ensure network safety, as it requires a comprehensive and adaptable security approach. These essential and adaptive measures are crucial for safeguarding the network from evolving and emerging threats that may compromise its integrity and functionality.

In the simulation of cognitive radio networks, the concept of Nash equilibrium is utilized to monitor the strategic choices made by both the Defender and Adversary, by

checking the Euclidean distance between current and previous strategies to determine the existence of a Nash equilibrium, and generating a message to notify the user when this condition is met. When the tolerance level is equal to 80 or above, the Nash equilibrium is achieved which is shown in Fig. 7.

The concept of Nash equilibrium is the bedrock of game theory and strategic decision-making, representing a state where both the Defender and Adversary find no incentive to alter their strategies. This equilibrium signifies a stable point reached through strategic interactions, where adjustments have been made to prevent any party from benefiting by changing their approach while the other party maintains their current strategy.

7 Conclusion and future work

The utilization of DSSS serves to strengthen communication robustness by spreading signals, thereby enhancing security. DSSS profoundly enhances the security state, thereby fortifying the network against adversarial interference. Within this dynamic landscape, the interaction between the Defender and Adversary takes on a strategic nature, with utilities and strategies fluctuating. The Defender adjusts resource allocation to protect the network, while the Adversary seeks to exploit vulnerabilities and maximize their benefits. Moments of strategic stability, known as Nash equilibrium checks, arise wherein neither party has an inclination to unilaterally alter their strategies. Despite providing strategic balance, Nash equilibrium does not guarantee optimal strategies, thereby emphasizing the necessity for adaptive security measures. The attainment of effective network security in cognitive radio networks necessitates continual adaptation, proactive measures, and resource allocation that promptly respond to emerging threats and vulnerabilities.

7.1 Future work

Possible future works in cognitive radio networks encompass the innovation of advanced security protocols and the incorporation of machine learning and artificial intelligence to detect threats in real-time and optimize resource allocation. In the realm of game theory, research can delve into intricate models and multi-player scenarios to strike a better balance between Defenders and Adversaries, all the while examining resilience against jamming attacks and techniques to mitigate interference. It is imperative to undertake cross-layer optimization, validate findings through experimentation in real-world settings, standardize efforts, and establish spectrum management policies to ensure the practical implementation of cognitive radio networks. Furthermore, exploring the ramifications of cognitive radio networks within the context of 5G and beyond, as well as delving into energy-efficient designs, present promising avenues for future exploration.

7.2 List of symbols and descriptions

Table 7 presents list of symbols used in this paper.

Table 7 List of symbols and descriptions

List of symbols	Description
N	The total number of users
M	The total number of channels
C, SF	The chip sequence and the spreading factor
X_b, X_a	The network states before and after DSSS
SS_b, SS_a	The security states before and after DSSS
S_d, S_a	Strategy of the Defender and Adversary in the Stackelberg game
$J_d(S_d, S_a), J_a(S_d, S_a)$	Objective functions of the Defender and Adversary in the Stackelberg game
λ, ρ	Scaling factors of the Defender and Adversary objective functions
$U_d(S_d, S_a), U_a(S_d, S_a)$	Utility of the Defender and Adversary in the Stackelberg game
R_i, A_i	Available resource allocation to the Defender and Adversary on channel (i)
S_D^{t+1}, S_A^{t+1}	Updated strategy of the Defender and Adversary in the Stackelberg game
SS_b, SS_a	Updated security states before and after DSSS

7.3 List of abbreviation

Table 8 shows the list of abbreviations with their meanings in alphabetical order.

Table 8 List of abbreviation and with their acronyms

	Meaning
CRNs	Cognitive radio networks
CSS	Cooperative spectrum sensing
DSSS	Direct sequence spread spectrum
DRL	Deep reinforcement learning
FH	Frequency hopping
NE	Nash equilibrium
PA	Power allocation
RA	Rate adaptation
SE	Stackelberg equilibrium
SS	Spectrum sensing
SUs	Secondary users

Acknowledgements

All authors have read and approved the published version of the manuscript.

Author contributions

M.I helped in conceptualization of the idea, development of the mathematical modeling, algorithm and simulation, writing, editing, and reviewing of the draft. P.Z worked in supervision and technical support throughout the entire draft. L.N supported in the research meetings and validation of simulations. M.S helped in technical support in modeling, simulations, writing, editing, and reviewing of the draft. F.M.B helped in participation in meetings and discussion.

Funding

Not available.

Availability of data and materials

Not applicable.

Declarations

Competing interests

The authors declare that they have no competing interests.

Received: 27 May 2024 Accepted: 13 August 2024

Published online: 17 September 2024

References

1. K.N. Vaishnavi, et al. A survey on jamming techniques in physical layer security and anti-jamming strategies for 6G, in *2021 28th International Conference on Telecommunications (ICT)* (IEEE, 2021)
2. M.F. Amjad et al., AdS: an adaptive spectrum sensing technique for survivability under jamming attack in cognitive radio networks. *Comput. Commun.* **172**, 25–34 (2021)
3. K. Ibrahim, et al. Bandwidth-efficient frequency hopping based anti-jamming game for cognitive radio assisted wireless sensor networks, in *2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring)* (IEEE, 2021)
4. A.K. Tiwari. Deep Reinforcement Learning based reliable spectrum sensing under SSDF attacks in Radio networks (2022)
5. V Shakhov, I Koo. Applying change point detection technique to dynamically support network security, in *2022 RIVF International Conference on Computing and Communication Technologies (RIVF)* (IEEE, 2022).
6. D.H. Tashman, W. Hamouda, An overview and future directions on physical-layer security for cognitive radio networks. *IEEE Netw.* **35**(3), 205–211 (2020)
7. A.H. Anwar, G. Atia, M. Guirguis, Adaptive topologies against jamming attacks in wireless networks: a game-theoretic approach. *J. Netw. Comput. Appl.* **121**, 44–58 (2018)
8. A. Garnaev, Y. Hayel, E. Altman. A Bayesian jamming game in an OFDM wireless network, in *2012 10th International Symposium on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt)* (IEEE, 2012).
9. M. Zou, et al. An evolutionary learning approach for anti-jamming game in cognitive radio confrontation, in *2022 IEEE International Conference on Systems, Man, and Cybernetics (SMC)* (IEEE, 2022)
10. L. Jia et al., Stackelberg game approaches for anti-jamming defence in wireless networks. *IEEE Wirel. Commun.* **25**(6), 120–128 (2018)
11. H. Fang, L. Xu, K.K.R. Choo, Stackelberg game based relay selection for physical layer security and energy efficiency enhancement in cognitive radio networks. *Appl. Math. Comput.* **296**, 153–167 (2017)
12. C. Chen et al., A game-theoretical anti-jamming scheme for cognitive radio networks. *IEEE Netw.* **27**(3), 22–27 (2013)
13. K. Ibrahim et al., Anti-jamming game to combat intelligent jamming for cognitive radio networks. *IEEE Access* **9**, 137941–137956 (2021)
14. B. Wang, Y. Wu, K.J.R. Liu, Game theory for cognitive radio networks: an overview. *Comput. Netw.* **54**(14), 2537–2561 (2010)
15. V. Navda, et al. Using channel hopping to increase 802.11 resilience to jamming attacks, in *IEEE INFOCOM 2007–26th IEEE International Conference on Computer Communications* (IEEE, 2007)
16. W. Xu, et al. The feasibility of launching and detecting jamming attacks in wireless networks, in *Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing* (2005)
17. W. Xu, et al. Channel surfing and spatial retreats: defenses against wireless denial of service, in *Proceedings of the 3rd ACM Workshop on Wireless security* (2004)
18. M. Strasser, et al. Jamming-resistant key establishment using uncoordinated frequency hopping, in *2008 IEEE Symposium on Security and Privacy (sp 2008)* (IEEE, 2008)
19. J. Zhang, et al. A practical SNR-guided rate adaptation, in *IEEE INFOCOM 2008—The 27th Conference on Computer Communications* (IEEE, 2008).
20. G. Noubir, et al. On the robustness of IEEE 802.11 rate adaptation algorithms against smart jamming, in *Proceedings of the Fourth ACM Conference on Wireless Network Security* (2011)
21. X. Wang et al., Dynamic spectrum anti-jamming communications: Challenges and opportunities. *IEEE Commun. Mag.* **58**(2), 79–85 (2020)
22. K. Pelechrinis, et al. Ares: an anti-jamming reinforcement system for 802.11 networks, in *Proceedings of the 5th International Conference on Emerging Networking Experiments and Technologies* (2009).
23. K. Ibrahim et al., Entice to trap: enhanced protection against a rate-aware intelligent jammer in cognitive radio networks. *Sustainability* **14**(5), 2957 (2022)
24. K. Pelechrinis, C. Koufogiannakis, S.V. Krishnamurthy, On the efficacy of frequency hopping in coping with jamming attacks in 802.11 networks. *IEEE Trans. Wirel. Commun.* **9**(10), 3258–3271 (2010)
25. M.K. Hanawal, M.J. Abdel-Rahman, M. Krunz, Joint adaptation of frequency hopping and transmission rate for anti-jamming wireless systems. *IEEE Trans. Mob. Comput.* **15**(9), 2247–2259 (2015)
26. Z. Quan, N. Yingtao, From adaptive communication anti-jamming to intelligent communication anti-jamming: 50 years of evolution. *Adv. Intell. Syst.* (2024). <https://doi.org/10.1002/aisy.202300853>
27. Z. Yupei, Z. Zhi-wen, Z. Shilian, Q. Fang, Intelligent anti-jamming decision with continuous action and state in bivariate frequency agility communication system. *IEEE Trans. Cogn. Commun. Netw.* (2023). <https://doi.org/10.1109/tccn.2023.3306363>
28. T.B. Nguyen, H.T. Dang, D.H. Le, T.H. Nguyen, P.K. Nguyen, X.Q. Nguyen. An adaptive channel selection scheme for anti-jamming radio communications (2023). <https://doi.org/10.1109/atc58710.2023.10318898>
29. W. Jinpeng, J. Wenyu, H. Kaizhi, S. Xiaoli, A communication anti-jamming scheme assisted by RIS with angular response. *Entropy* (2023). <https://doi.org/10.3390/e25121638>

30. N. Yingtao, Pu. Ziming, Anti-jamming communication using slotted cross Q learning. *Electronics* (2023). <https://doi.org/10.3390/electronics12132879>
31. Y. Bai et al., Sample-efficient learning of Stackelberg equilibria in general-sum games. *Adv. Neural. Inf. Process. Syst.* **34**, 25799–25811 (2021)
32. M. Abdallah, et al. The effect of behavioral probability weighting in a sequential defender-attacker game, in *2020 59th IEEE Conference on Decision and Control (CDC)* (IEEE, 2020).
33. M. Pirani et al., A graph-theoretic equilibrium analysis of attacker-defender game on consensus dynamics under \mathcal{H}_2 performance metric. *IEEE Trans. Netw. Sci. Eng.* **8**(3), 1991–2000 (2020)

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Terms and Conditions

Springer Nature journal content, brought to you courtesy of Springer Nature Customer Service Center GmbH (“Springer Nature”).

Springer Nature supports a reasonable amount of sharing of research papers by authors, subscribers and authorised users (“Users”), for small-scale personal, non-commercial use provided that all copyright, trade and service marks and other proprietary notices are maintained. By accessing, sharing, receiving or otherwise using the Springer Nature journal content you agree to these terms of use (“Terms”). For these purposes, Springer Nature considers academic use (by researchers and students) to be non-commercial.

These Terms are supplementary and will apply in addition to any applicable website terms and conditions, a relevant site licence or a personal subscription. These Terms will prevail over any conflict or ambiguity with regards to the relevant terms, a site licence or a personal subscription (to the extent of the conflict or ambiguity only). For Creative Commons-licensed articles, the terms of the Creative Commons license used will apply.

We collect and use personal data to provide access to the Springer Nature journal content. We may also use these personal data internally within ResearchGate and Springer Nature and as agreed share it, in an anonymised way, for purposes of tracking, analysis and reporting. We will not otherwise disclose your personal data outside the ResearchGate or the Springer Nature group of companies unless we have your permission as detailed in the Privacy Policy.

While Users may use the Springer Nature journal content for small scale, personal non-commercial use, it is important to note that Users may not:

1. use such content for the purpose of providing other users with access on a regular or large scale basis or as a means to circumvent access control;
2. use such content where to do so would be considered a criminal or statutory offence in any jurisdiction, or gives rise to civil liability, or is otherwise unlawful;
3. falsely or misleadingly imply or suggest endorsement, approval, sponsorship, or association unless explicitly agreed to by Springer Nature in writing;
4. use bots or other automated methods to access the content or redirect messages
5. override any security feature or exclusionary protocol; or
6. share the content in order to create substitute for Springer Nature products or services or a systematic database of Springer Nature journal content.

In line with the restriction against commercial use, Springer Nature does not permit the creation of a product or service that creates revenue, royalties, rent or income from our content or its inclusion as part of a paid for service or for other commercial gain. Springer Nature journal content cannot be used for inter-library loans and librarians may not upload Springer Nature journal content on a large scale into their, or any other, institutional repository.

These terms of use are reviewed regularly and may be amended at any time. Springer Nature is not obligated to publish any information or content on this website and may remove it or features or functionality at our sole discretion, at any time with or without notice. Springer Nature may revoke this licence to you at any time and remove access to any copies of the Springer Nature journal content which have been saved.

To the fullest extent permitted by law, Springer Nature makes no warranties, representations or guarantees to Users, either express or implied with respect to the Springer nature journal content and all parties disclaim and waive any implied warranties or warranties imposed by law, including merchantability or fitness for any particular purpose.

Please note that these rights do not automatically extend to content, data or other material published by Springer Nature that may be licensed from third parties.

If you would like to use or distribute our Springer Nature journal content to a wider audience or on a regular basis or in any other manner not expressly permitted by these Terms, please contact Springer Nature at

onlineservice@springernature.com